СТРУЧНИ ЧЛАНЦИ
ПРОФЕССИОНАЛЬНЫЕ СТАТЬИ
PROFESSIONAL PAPERS

APPLICATION OF MULTIPLE CRITERIA DECISION MAKING IN THE SELECTION OF DIGITAL FORENSICS SOFTWARE

Dejan R. Stanivuković[a], *Dragan* M. Ranđelović[b]
[a] Serbian Armed Forces, General Staff, Military Police Department, Crime - Investigation Group, Novi Sad, Republic of Serbia,
e-mail: stanivuk@nscable.net,
ORCID iD: http://orcid.org/0000-0002-3605-5527,
[b] Ministry of the Interior, Academy of Criminalistic and Police Studies, Department of Information Technologies, Belgrade, Republic of Serbia,
e-mail: dragan.randjelovic@kpa.edu.rs,
ORCID iD: http://orcid.org/0000-0002-2008-4729

DOI: 10.5937/vojtehg64-8938
FIELD: Computer Science, Information Technologies
ARTICLE TYPE: Professional Paper
ARTICLE LANGUAGE: English

Abstract:

Nowadays there is almost no criminal offense in the investigation of which digital evidence does not play a key role. Constant increase of the capacity of media that store digital data leads to continuous increase of the time necessary to identify and copy (acquire) digital evidence. Selection of appropriate digital forensics software is gaining in importance.

Selection of adequate software includes a previous comparative analysis of two or more digital forensics software tools and an optimization process. The objective of the comparative analysis of these software tools is to determine and compare each of their realistic and comparable performances. Optimization aims to determine which of digital forensics software tools has better performances.

This paper shows one of possible variants of selecting digital forensics software, using the latest scientific achievements in support of decision making based on the analytic hierarchy process (AHP) method and the Expert Choice computer program.

Key words: *forensics software, digital forensics, expert choice, optimization, digital evidence, comparative analysis.*

Introduction

The implementation of a high-quality comparative analysis of standard digital forensics software is a very complex task. A qualitative analysis involves a larger number of the latest software programs to be analysed. Since commercial software is rather expensive (McClure, et al., 2002, p.614) this adds to the complexity of the problem.

In addition, there is a problem regarding professional usage and experience in working with selected software. In under-developed and developing countries, such as the Republic of Serbia, which consider using digital forensics, there are practically no certified digital forensic experts. This points to another significant problem.

Continuous development of digital forensics software and daily improvements of their characteristics through new software versions and generations make the results of these analyses "short of breath". This imposes a need to base the selection of the optimal digital forensics software on a preliminary analysis and a comparison of more digital forensics software tools of the latest generation, which is often not economically feasible and sometimes not even possible.

Such problems can be overcome in many ways. In this sense, there are the results of comparative analyses of digital forensics software published in the scientific literature and the results published in peer-reviewed journals with a long tradition of comparative analyses. Both methods have their positive and negative sides.

A positive characteristic of the results of comparative analyses of digital forensics software published in the scientific literature is comprehensiveness and scientific foundation while a negative side is that they are often not up-tp-date due to the development of new versions of software. A positive characteristic of the results of professional journals with a long tradition of comparative analyses of such software is the up-to-dateness of software choice while a negative side is a populistic approach to the analysis due to different educational profiles of readers.

A comparative analysis of standard software programs of digital forensics, viewed from the perspective of this study, is a function of defining elements and indicators necessary to optimize the selection of digital forensics software and to present the optimization process itself. In accordance with the prevailing opinion of the scientific and professional community, standard digital forensics software products are from American Guidance Software and Data Access as well as from German X-Ways, i.e. their digital forensics software tools named EnCase, FTK (FTK Imager) and WinHex. The problem of securing legal software necessary for comparative analyses is overcome by using their older test, demo, and lite versions ie. versions EnCase Enterprise v4, FTK v1.81.6 (FTK Imager 3.1.1.) and WinHex 18.5.

These versions of digital forensics software are limited in terms of some advanced features and scope of analysis but not in their primary functions which are identifying and copying (acquisition) of disks. These functions are also the subject of analysis.

Specifying the above digital forensics software also defines the alternatives for optimization. The first step in the optimization process is to determine the optimization objective. In the scientific and professional literature it is often stressed that EnCase, FTK and WinHex have similar features i.e. performances. In order to determine which of the above software programs has better performance, optimization is used to identify an alternative that, according to the established criteria, has better basic possibilities or primary performances. In this sense, the objective of optimization is defined as" Selection of Digital Forensics Software with better primary performances". In short, to optimize means to make the best decision when choosing between alternatives, comparing them with each other according to certain criteria.

The selection of criteria is determined by the optimization objective. In this case, criteria must be chosen to reflect performances. The operating software speed when performing functions that precede the analysis (of primary functions), expressed in the units of time, is certainly one of the most important performances. "Live disk" Identification speed for its preliminary analysis is important in taking emergency measures in a process such as making a decision on the detention of the suspect. On the other hand, the speed of making "live disk" copies for its detailed analysis is important in taking measures to detain the suspect, where the time available to collect evidence and submit it to the judge for preliminary proceedings is limited to 48 hours. Since today's disk capacity is measured in Terabytes (TB) and larger units of measurement, it is important to note that the process of disk copying may take considerable time. According to some authors, the length of time required to create copies of a disk, in addition to capacity, is affected by the speed at which the network cable transfers data contained on the disk (Simeunović, Ristić, 2013, p.1009).

A selection of digital forensics software tools for digital forensic investigation gains in significance due to the fact that digital forensics software preparation, including the selection of appropriate software, stands out as a new phase of digital forensic investigation that precedes and affects other phases: evidence collection and examination, analysis and reporting (Delija, 2015). Evaluation and selection of tools for digital forensic investigation is still a challenge and it is an insufficiently researched topic in the field of digital forensics. The selection of appropriate tools to be used for digital forensic investigation greatly influences the outcome in court. While the goal is clear - to obtain valid digital evidence acceptable in court, in practice it appears that this is not easy to achieve at all (Kaurin, Anucojić, 2012, p.715).

Comparative analysis of standard digital forensics software

Based on author's own experience, the optimization criteria are: (1) identification of the disk, and (2) copying the disk. Each of these criteria is evaluated using three sub-criteria: (1.1) time for the identification of the 1 GB flash disk, (1.2) time for the identification of the 4 GB flash disk and (1.3) time for the identification of the 8 GB flash disk, (2.1) time for copying the 1 GB flash disk, (2.2) time for copying the 4 GB flash disk, and (2.3) time for copying the 8 GB flash disk.

Based on the values obtained by testing the Digital Forensics software EnCase Enterprise v4, FTK v1.81.6 and WinHex 18.5, in terms of the time necessary to identify the flash disks of 1, 4 and 8 GB, it is evident that EnCase and WinHex software, under the same conditions (Table 1), identify the disk in less than one second, or give proportional values which remain the same when the disk capacity is changed (Table 2).

On the other hand, under the same conditions, FTK software takes some time to identify the disk, i.e. gives slow progressive values that grow with the increase of the disk capacity but at a smaller ratio compared to the disk capacity increase (Table 2).

Table 1 – Conditions of testing the digital forensics software: EnCase, FTK and WinHex, in terms of the time required to identify disks of 1, 4 and 8 GB
Таблица 1 – Условия, в которых испытаны программные обеспечения цифровой форензики EnCase, FTK и WinHex, с учетом времени, необходимого для идентификации накопителя 1, 4 и 8 GB
Tabela 1 – Uslovi u kojima su testirani softveri digitalne forenzike EnCase, FTK i WinHex, sa aspekta vremena neophodnog za identifikaciju diskova od 1,4 i 8 GB

Computer configuration:	***Windows edition – Windows XP Profesional (SP3)***
	System manufacturer – Acer
	System processor–Intel(R)Pentium(R)DualCPU E2220@2.4 GHz
	Installed memory (RAM) – 768 MB
	System type – 32-bit Operating System
Alternative:	***EnCase Enterprise v4***
	FTK v1.81.6
	WinHex 18.5
Criterion:	***identification speed disk***
Sub-criteria:	***flash disk Kingston DTI/1GB***
	flash disk SanDisk Cruzer Edge 4 GB
	flash disk Kingston DT101 G2 8 GB

Table 2 – Display of the values obtained by testing the digital forensics software: EnCase, FTK and WinHex, in terms of the time required to identify disks of 1, 4 and 8 GB
Таблица 2 – Изображение значений, полученных путем тестирования программного обеспечения цифровой форензики EnCase, FTK и WinHex, с учетом времени, необходимого для идентификации накопителя 1, 4 и 8 GB
Tabela 2 – Prikaz vrednosti dobijenih testiranjem softvera digitalne forenzike EnCase, FTK i WinHex, sa aspekta vremena neophodnog za identifikaciju diskova od 1,4 i 8 GB

No.	IDENTIFICATION DISK	EnCase Enterprise v4	FTK v1.81.6	WinHex 18.5	Difference		
					EC/FTK	EC/WH	FTK/WH
1	Kingston DTI/1GB 	< 00:00:01	00:01:02	< 00:00:01	61	0	61
2	SanDisk Cruzer Edge/4 GB 	< 00:00:01	00:03:50	< 00:00:01	229	0	229
3	Kingston DT101G2/8 GB 	< 00:00:01	00:05:01	< 00:00:01	300	0	300

It is important to notice that the values in Table 2 are not unique since all forensic software programs, to a lesser or greater extent, have special options that are automatically executed. Since it is not possible to deactivate all the options, the given values should be regarded only as an indication to select the right forensic software for a particular case.

When it comes to the differences in the values obtained by testing the EnCase and FTK software tools, expressed descriptively, it is evident that it is: "moderately to very important" in favour of EnCase software for the 1 GB (61 s) disk; "very important to extremely important" in favour of EnCase software for the 4 GB (229 s) disk and "extremely important" in favour of EnCase software for the 8 GB (300 s) disk. The case is identical when it comes to the difference between FTK and WinHex software, in favor of WinHex. Bearing in mind that EnCase and WinHex software tools give equal values when tested, regardless of the disk size, their values are "equally important". The aforementioned descriptive expression is necessary in order to adjust the difference of the results obtained by testing to the text assessment scale of Expert Choice program, which will be diskussed further on.

Based on the values obtained by testing the Digital Forensics software EnCase Enterprise v4, FTK Imager 3.1.1. and WinHex 18.5, in terms of time required to copy the flash disks of 1, 4 and 8 GB, it is evident that the EnCase software tool, under the same conditions (Table 3), with the increase of the disk capacity, gives first slow progressive values that grow with the disk capacity increase but at a smaller ratio compared to the disk capacity increase; with further disk capacity increase, its values become rapidly progressive and grow with the increase of the disk capacity at a greater ratio compared to the disk capacity increase (Table 4).

On the other hand, the FTK software tool, under the same conditions (Table 3), provides constantly accelerated progressive values that grow

with the increase of the disk capacity at a greater ratio compared to the disk capacity increase (Table 4).

The WinHex software tool, under these conditions (Table 3), changes the values identically to EnCase software; the only difference is that the progression and increase of these values are less pronounced with the disk capacity increase (Table 4).

Table 3 – Conditions under which digital forensics software tools -EnCase, FTK and WinHex- are tested, in terms of the time required to copy the disks of 1, 4 and 8 GB
Таблица 3 – Условия, в которых испытаны программные обеспечения цифровой форензики EnCase, FTK и WinHex, с учетом времени, необходимого для создания копии дисков 1, 4 и 8 GB
Tabela 3 – Uslovi pod kojima su testirani softveri digitalne forenzike EnCase, FTK i WinHex, sa aspekta vremena neophodnog za izradu kopija diskova od 1,4 i 8 GB

Computer configuration:	***Windows edition – Windows XP Profesional (SP3)***
	System manufacturer – Acer
	System processor–Intel(R)Pentium(R)DualCPU 2.4 GHz
	Installed memory (RAM) – 768 MB
	System type – 32-bit Operating System
Alternative:	***EnCase Enterprise v4***
	FTK Imager 3.1.1.
	WinHex 18.5
Criterion:	***the speed of making copies of a disk***
Sub-criteria:	***flash disk Kingston DTI / 1GB***
	flash disk SanDisk Cruzer Edge / 4 GB
	flash disk Kingston DT101 G2 / 8 GB

Table 4 – Display of the values obtained by testing digital forensics software tools -EnCase, FTK and WinHex - in terms of the time required to copy the disks of 1, 4 and 8 GB
Таблица 4 – Изображение значений, полученных путем тестирования программного обеспечения цифровой форензики EnCase, FTK и WinHex, с учетом времени, необходимого для создания копии дисков 1, 4 и 8 GB
Tabela 4 – Prikaz vrednosti dobijenih testiranjem softvera digitalne forenzike EnCase, FTK i WinHex, sa aspekta vremena neophodnog za izradu kopija diskova od 1,4 i 8 GB

No.	DISK DUPLICATION	EnCase Enterprise v4	FTK Imager 3.1.1.	WinHex 18.5	Difference		
					EC/FTK	EC/WH	FTK/WH
1	*Kingston DTI/1GB* 	00:01:34	00:01:22	00:01:28	12	6	6
2	*SanDisk Cruzer Edge/4 GB* 	00:04:50	00:06:00	00:05:45	70	55	15
3	*Kingston DT101G2/8 GB* 	00:13:49	00:14:44	00:11:22	55	147	202

The difference in the values obtained by testing the EnCase and FTK software tools, expressed descriptively, is the following: for the disk of 1 GB (12 s) it is "moderately important" in favor of FTK software; for the disk of 4 GB (70 s) it is "very important" in favour of EnCase software and for the disk of 8 GB (55 s) it is "moderately to very important" in favour of EnCase software.

The difference in the values obtained by testing EnCase and WinHex software, expressed descriptively, is the following: for the disk of 1 GB (6 s) it is "equally to moderately important" in favour of WinHex software; for the disk of 4 GB (55 s) it is "moderately to very important" in favour of EnCase software and for the disk of 8 GB (147 s) it is "very to extremely important" in favour of WinHex software.

The difference in the values obtained by testing FTK and WinHex software, expressed descriptively, is the following: for the disk of 1 GB (6 s) it is "equally to moderately important“ in favor of FTK software; for the disk of 4 GB (15 s) it is "moderately important" in favour of WinHex software and for the disk of 8 GB (202 s) it is "extremely important" in favour of WinHex software.

Optimizing Digital Forensics Software Selection

In the process of optimization, decision-makers have access to the latest scientific achievements in support of decision making. One of such developments is the analytic hierarchy process (AHP) method. This method was developed by Thomas Saaty in the early seventies in order to assist decision-makers in solving complex problems of decision making with multiple criteria and the presence of a large number of alternatives. The AHP method allows decision-makers to include a subjective attitude, experience, knowledge and intuition in decision making.

The AHP presents complex problems through a model in the form of hierarchy. Each level consists of several elements, where the elements of the same level are independent of each other but comparable. In today's conditions, the AHP method is applied by means of the Expert Choice 2011 computer program (hereinafter: EC 2011). This computer program was developed by a well-known manufacturer of computer programs, the Decision Support Software Company. It is such an important product that a part of the company was named later by this computer program - Expert Choice (Čupić, et al., 1992, p.131).

The process of using EC 2011 program includes the following phases: defining the objective; defining (generating) alternatives; defining criteria and sub-criteria (structuring the problem); comparing the criteria in relation to the objective (determining the influence of the criteria on the objective); comparing the sub-criteria with the criteria (determining the influence of the sub-criteria on the criteria); comparing alternatives in relation to the sub-criteria (determining the relative impact of each alternative on a particular sub-criterion); synthesis of the alternatives regarding the objective (aggregation of the solution) and a sensitivity analysis (Fakultet organizacionih nauka, 2015).

In the phase of defining the objective, it is necessary to enter a description of the previously defined objective "DIGITAL FORENSICS SOFTWARE SELECTION" into the relevant program window.

In the phase of defining alternatives, it is necessary to enter the data on the alternatives under consideration, or the names of the three leading digital forensics software programs selected based on the opinions of professional and scientific community, "EN CASE", "FTK" and "WIN HEX". A more detailed description of the objective is preferable in order to continually point to the purpose of optimization - "The comparison of the leading digital forensics software programs selected based on the opinions of professional and scientific community, in order to identify the one with better primary performances" (Figure 1).

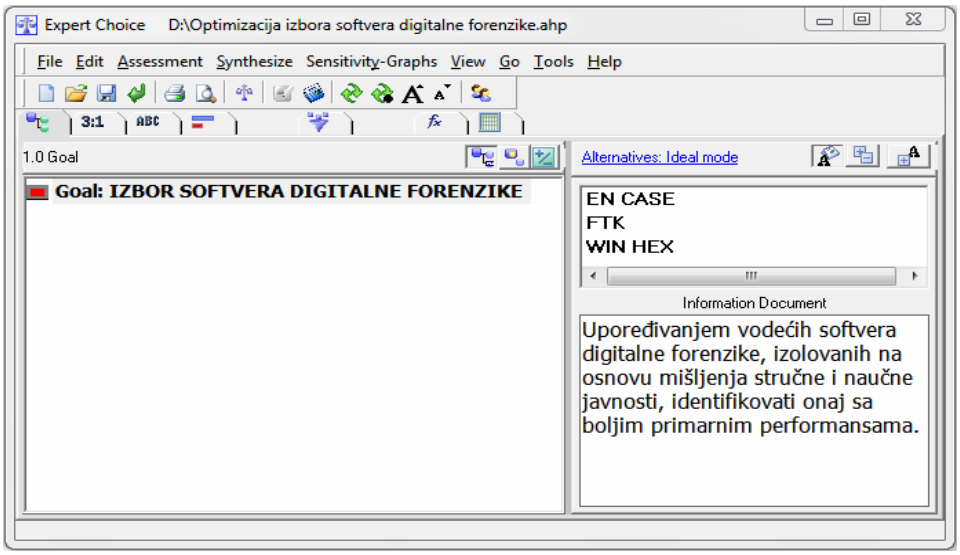

Figure 1 – Definition of alternatives and a detailed description of the objective
Рис. 1 – Определение альтернатив и подробное описание цели
Slika 1 – Definisanje alternativa i detaljno opisivanje cilja

In the stages of defining criteria and sub-criteria, the hierarchy is structured (Figure 2), and it is necessary to enter the data on criteria - "DISK IDENTIFICATION" and "DISK COPYING" and the information on sub-criteria: 1 GB flash disk, 4GB flash disk and 8 GB flash disk in the form of "disk 1", "disk 4" "disk 8" (Figure 3).

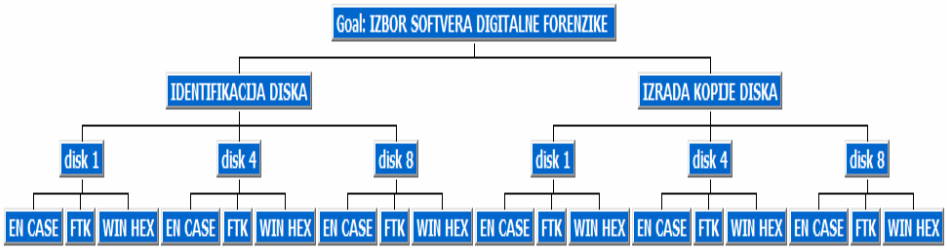

Figure 2 – Hierarchical structure of the problem of digital forensics software selection
Рис. 2 – Иерархическая структура проблемы выбора программного обеспечения цифровой форензики
Slika 2 – Hijerarhijska struktura problema izbora softvera digitalne forenzike

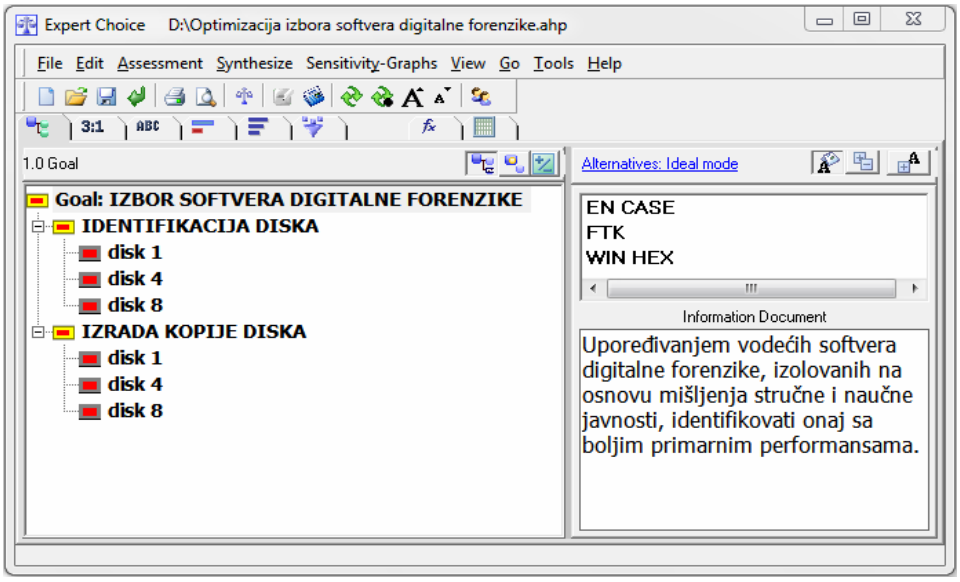

Figure 3 – Defining criteria and sub-criteria in EC 2011 program
Рис. 3 – Определение критериев и субкритериев в программе EC 2011
Slika 3 – Definisanje kriterijuma i potkriterijuma u programu EC 2011

In the phase of comparing the criteria in relation to the objective, their weight ratios are assessed in relation to the objective by comparing pairs of criteria with the help of textual descriptions of the levels of importance of one over the other[1], taking into account the index inconsistencies[2] in the assessment criteria.

Upon completion of the comparison of the criteria to the objective and the sub-criteria in relation to the criteria, EC 2011 program expresses each criteria/sub-criteria weight factor (importance) to the object, or the criterion (Figure 4). When the criteria are compared, the criterion of "DISK COPYING" (0.800) is more important than the criterion of "DISK IDENTIFICATION" (0.200). In comparison with other sub-criteria (in the case of both criteria) the most important sub-criterion is "disk 8" (0.147 / 0.588), followed by sub-criterion "disk 4" (0.041 / 0.165) and the least important is sub-criterion "disk 1" (0.012 / 0.046). The resulting weights indicate that EC 2011 followed the decision-maker's will.

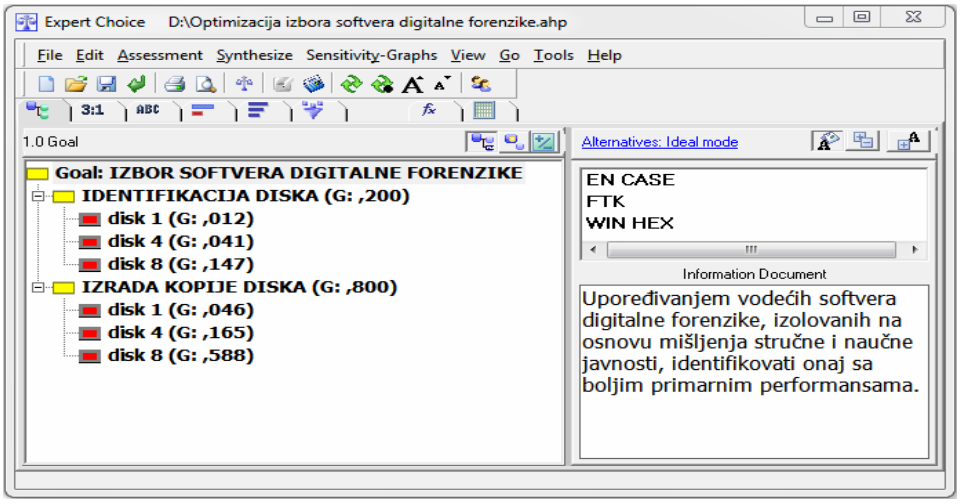

Figure 4 – Weights of criteria (sub-criteria) compared to the objective (criterion)
Рис. 4 – Вес коэффициента критериев (субкритериев) к объекту (критерий)
Slika 4 – Težinski koeficijenti kriterijuma (potkriterijuma) u odnosu na cilj (kriterijum)

[1] Equal (criteria that are being compared are of the same importance), Moderate (one criterion is moderately more important than the other), Strong (one criterion is significantly more important than the other), Very Strong (one criterion is quite significantly more important than the other) i Extreme (one criterion is extremely more important than the other).

[2] Inconsistency (lat. inconsistentia) transience, impermanence, incongruity, contradiction, diskrepancy.

Regarding the obtained results (coefficients), it is important to note that EC 2011 was guided by the expressed will of decision-makers (evaluators). It is this feature of EC 2011 that allows decision-makers to create basic optimization parameters according to their interests and needs. At the stage of comparing alternatives to the sub-criteria, unlike the previous phase of comparing the criteria and the sub-criteria, comparing alternatives is based on the quantitative indicators obtained by testing, with a free will of decision-makers completely excluded.

Given the above, before comparing alternatives, it is necessary to adjust the results obtained by testing to the text assessment scale of the EC 2011 program (Table 5). It should be noted that the 2011 EC program allows mutual comparison and evaluation of: the criteria in relation to the objective; the sub-criteria with respect to the criteria, or the alternatives with respect to the sub-criteria in different modes (options). In addition to the text mode (option "ABC") decision-makers can use a graphical mode (option "ıı"), or a numeral mode (option "3:1"). These modes of comparison correspond to preferences of decision-makers who can express themselves better either with numbers, words or visually.

Table 5 – Results obtained by testing adapted to the text scale of the EC 2011 program
Таблица 5 – Результаты, полученные путем тестирования, приспособленные пользовательской шкале программы EC 2011
Tabela 5 – Rezultati dobijeni testiranjem prilagođeni tekstualnoj skali programa EC 2011

РЕЗУЛТАТ	ЕКВИВАЛЕНТ	ТЕКСТУАЛНА СКАЛА	ЗНАЧЕЊЕ
300	→	*Extreme*	- екстремно значајно
229	→	-	- веома јако до екстремно значајно
202	→	*Very Strong*	- веома јако значајно
147	→	-	- јако до веома јако значајно
70	→	*Strong*	- јако значајно
55	→	-	- умерено до јако значајно
15	→	*Moderate*	- умерено значајно
6	→	-	- једнако до умерено значајно
0	→	*Equal*	- једнако значајно
6	→	-	- једнако до умерено значајно
15	→	*Moderate*	- умерено значајно
55	→	-	- умерено до јако значајно
70	→	*Strong*	- јако значајно
147	→	-	- јако до веома јако значајно
202	→	*Very Strong*	- веома јако значајно
229	→	-	- веома јако до екстремно значајно
300	→	*Extreme*	- екстремно значајно

The results obtained by testing are adapted to the text scale of the EC 2011 program in such a way that the smallest value obtained by testing (0 s) is equal to the minimum value of the text scale of the program (equal) and

the maximum value obtained by testing (300 s) is equal to the highest value of the text scale of the program (extreme). The values between the minimum and maximum values obtained by testing, depending on their size, are equal to the corresponding values of the text scale of the program.

The technique of evaluating alternatives with respect to the sub-criteria, with the exception of the free will of decision-makers, is identical to the previously described technique of assessing the criteria in relation to the objective, or the sub-criteria with respect to the criteria. After the assessment of the significance of alternatives with respect to all sub-criteria, by positioning to "DIGITAL FORENSICS SOFTWARE SELECTION", the EC 2011 program shows the weights (importance) with respect to the objective for each alternative (Figure 5).

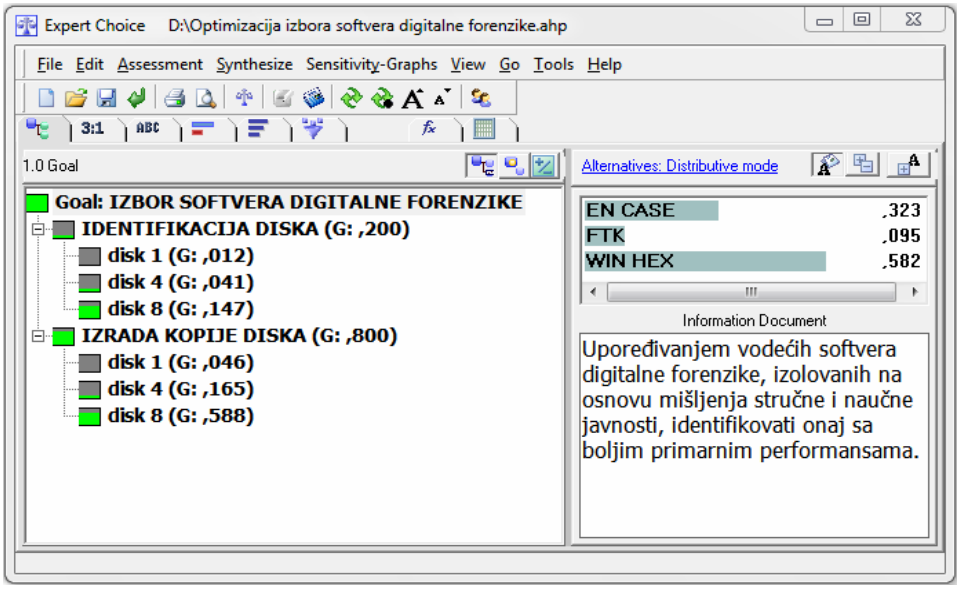

Figure 5 – Weights of alternatives in relation to the objective
Рис. 5 – Весовые коэффициенты альтернатив цели
Slika 5 – Težinski koeficijenti alternativa u odnosu na cilj

When comparing alternatives in relation to the objective, the most important is the alternative "WIN HEX" (0.582), less important is the alternative "EN CASE" (0.323) and the least important is the alternative "FTK" (0.095). In the phase of the synthesis of alternatives with respect to the objective, selecting the With Respect to Goal option in the Synthesize menu results in a graph of the expected alternative values with respect to the objective (Figure 6).

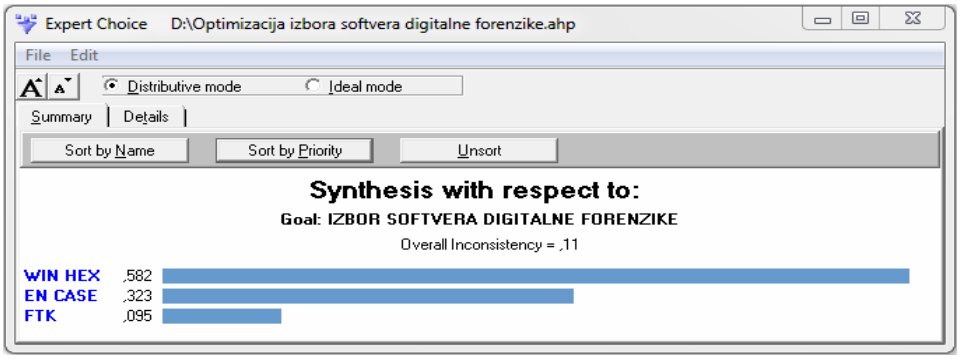

Figure 6 – Graph of the anticipated alternatives in relation to the objective
Рис. 6 – Диаграмма предполагаемых альтернатив цели
Slika 6 – Graf očekivanih alternativa u odnosu na cilj

In the final analysis, digital forensics software with the best performance is the primary software "WIN HEX" (0.582).

In the phase of the sensitivity analysis, four graphic forms of the sensitivity analysis of the obtained results can be used. These forms are accessed from the Sensitivity Graphs menu: performance analysis (Performance option), analysis of the impact of each individual criterion on the final solution (Gradient option), analysis of para-alternatives with all their criteria "forehead to forehead"(Head to Head option) and dynamic analysis (Dynamic option) as well as the possibility to simultaneously display all four graphs (Open Four Graphs option). The sensitivity analysis of the obtained results was carried out by the Dynamic option in the Sensitivity Graphs menu that can monitor changes in the priorities of other criteria and alternatives (Figure 7).

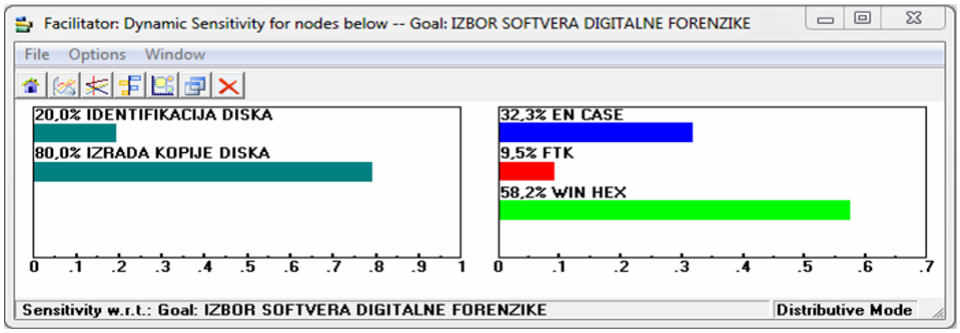

Figure 7 – Graph of the dynamic analysis
Рис. 7 – График динамического анализа
Slika 7 – Grafik dinamičke analize

During the dynamic analysis, changing the weights of multiple criteria distorts the initial bases of the criteria priorities which results in the creation of new alternative priorities. If small changes in weight for multiple criteria lead to a shift in priorities for alternatives, it is considered that the obtained solution is sensitive and, in this case, the first two ranked solutions should equally be taken into account in the selection of the final solution. Otherwise, it is considered that the solution is not sensitive and, as such, final.

In order to check sensitivity, a significant change in the priority of the "DISK IDENTIFICATION" criterion has been done from 20.0% to 80.0%, when the program automatically calculates the values of the change of the "DISK COPYING" criterion priority from 80.0% to 20.0%. It is also automatically shown how these changes affect the change in the value of the priority of alternatives. In this case, the change of the criteria priority has led only to a change in the alternative value: "WIN HEX" alternative was changed from 58.2% to 49.9%, "EN CASE" alternative from 32.3% to 43.4% and "FTK" alternative from 9. 5% to 6.7%.

Bearing in mind that changing the criteria priority did not lead to changes in the priority of alternatives, i.e. that the best solution is still the "WIN HEX" alternative (Figure 8), it is considered that the obtained solution is not sensitive to changes, and, as such, is the final selection.

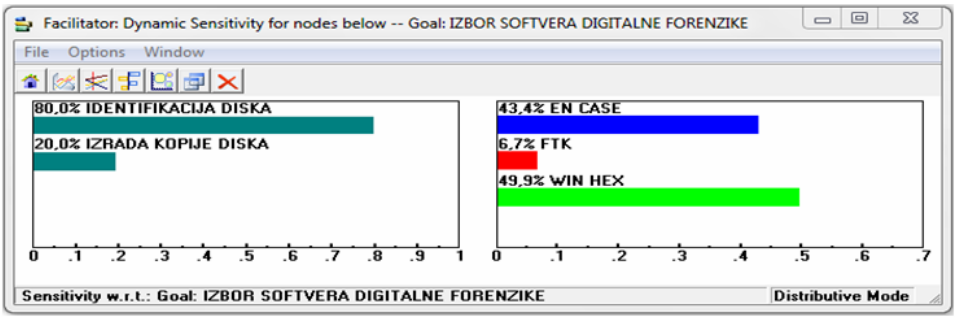

Figure 8 – Revised graph of the dynamic analysis - the "DISK IDENTIFICATION" criterion
Рис. 8 – Измененные графики динамического анализа - по критерию "ИДЕНТИФИКАЦИЯ ДИСКА"
Slika 8 – Izmenjeni grafik dinamičke analize – po kriterijumu „IDENTIFIKACIJA DISKA"

This model is applicable in the case of a large number of criteria, sub-criteria and alternatives. Randjelovic's (2011, pp. 112-113) comparative analysis of the authenticity and the verification of forensic tools EnCase, FTK Sleuth Kit with Autopsy browser shows a possibility of structuring the problem in the EC 2011 program in the case of a large number of alternatives, criteria and sub-criteria (Figure 9).

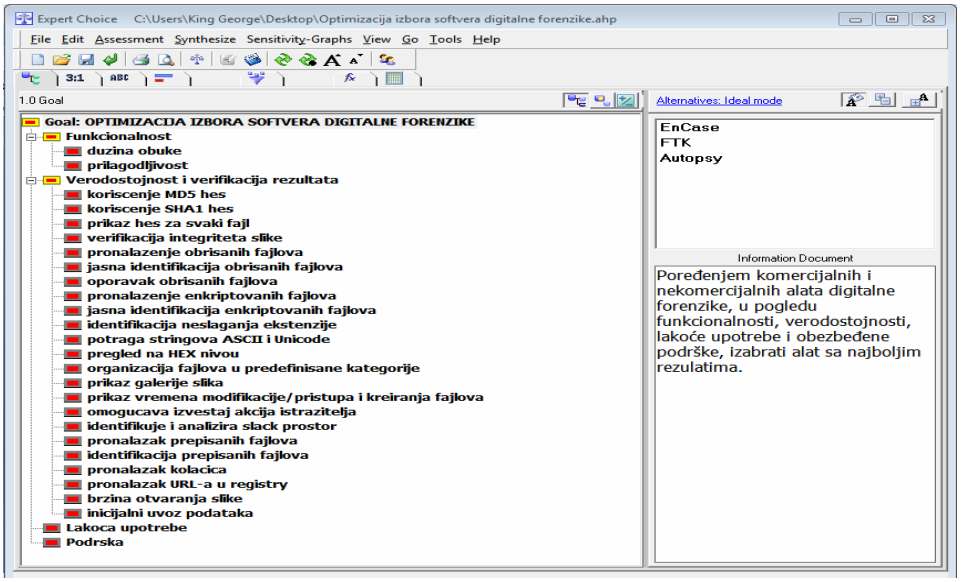

Figure 9 – Example of structuring a problem in EC 2011 with a large number of alternatives, criteria and sub-criteria
Рис. 9 – Пример структурирования проблемы в программе EC 2011 при большом количестве альтернатив, критериев и субкритериев
Slika 9 – Primer strukturiranja problema u programu EC 2011 pri većem broju alternativa, kriterijuma i potkriterijuma

Conclusion

This paper presents a model of selecting digital forensics software using most advanced scientific achievements in support of decision making based on the method of the analytic hierarchy process. One of the major problems in the application of this method is to define criteria and the evaluation of their relative weights. The authors have defined criteria and assessed the values of their relative weights based on their own experience gained in previous scientific research and practical investigation of crimes of cybercrime.

A precise procedure of this method implementation has resulted in the following order of alternatives in the model: "EN CASE" (first alternative) - 0.323 (second in the ranking), "FTK" (second alternative) - 0,095 (third in the ranking) and "HEX WIN" (third alternative) - 0.582 (first in the ranking). Particularly significant is the fact that changing the criteria priority does not lead to changes in the priority of alternatives, i.e. that the solution obtained is not sensitive to changes.

The first alternative has the highest rank (0.582), which is why it is the best or the optimal one. This alternative is also acceptable with

regard to the disk identification criterion and the disk copying criterion, i.e. this alternative enables the shortest time for the identification and copying of digital evidence. The advantage of this alternative is particularly evident with the increase of the treated disk capacity.

The second alternative in the rank has a lower value (0.323) which makes it less favorable. A change in the criteria priority does not lead to a change in alternative priority, but further increases the value of this alternative. This alternative is acceptable according to the criterion of disk identification but not according to the criterion of disk copying; namely, this alternative enables fast identification without securing digital evidence – this drawback is more pronounced with the increase of the treated disk capacity.

The third alternative in the rank has a minimum value (0.095), which is why it is the least favorable. This alternative is not acceptable either according to the criterion of disk identification or according to the criterion of disk copying, i.e. this alternative does not enable fast identification and provision of digital evidence - this disadvantage is more pronounced with increasing the capacity of the treated disk.

This conclusion applies only to the results of the tests carried out for this study. The choice is narrowed down to mainly older versions of Digital Forensics EnCase, FTK and a newer version of WinHex software and their performances in disk identifying and copying.

Some software tools, such as FTK and, in certain segments, EnCase, have options that cannot be deactivated and which are not necessary for the disk identification and copying and which further extend these processes. These background processes are the reason why for FTK software it is not possible to predict the time required to copy the disk, while the estimated copy time for EnCase is unreliable. Unlike the aforementioned software tools, WinHex provides accurate time necessary to copy a particular disk and warns the investigator if it is very long.

At the same time, the background processes carried out by FTK improve its performance in the next phases of digital forensic investigations, such as disk search and analysis. Significant advantages of FTK are the functions to filter files in order to distinguish irrelevant (system) files from the relevant (evidence) files, as well as a possibility of decryption of encrypted files. This software is considered to be the best software for searching and analysis of electronic messages (e-mails).

On the other hand, for the same phases of the investigation, EnCase and WinHex use software modules (scripts) for the automation of individual research. In addition to this, a significant advantage of these software tools is a possibility to search disks of virtually unlimited capacity.

All of these and many other advantages of particular software tools, both common and specific ones, are essential for a thorough and complete digital forensic investigation. For this reason, for the needs of particular digital forensic investigations, it is necessary to choose and use

the optimal digital forensics software for each stage of the investigation, taking into account that optimization criteria and sub-criteria should meet the needs of individual stages of the investigation.

It is important to mention that this is the case of an optimization model with a minimum number of alternatives, criteria and sub-criteria, from the viewpoint of the entire digital forensic investigation. Consideration of a large number of alternatives, criteria and sub-criteria and each individual phase of the investigation makes an analysis and an optimization more complicated but guarantees better results and, therefore, a more thorough and complete digital forensic investigation.

References

Čupić, M., Novaković, T., & Svilar, M., 1992, *Generatori i aplikacije sistema za podršku odlučivanju*, Beograd: Naučna knjiga, p.131.

Delija, D., 2015, [Internet], Available at: <http://www.slideshare.net/DamirDelijadamirdeli/racunalna-forenzika-osvrt-prezentacija-16399162 2015>, Retrieved: 18.04.2015.godine.

Fakultet organizacionih nauka Beograd, 2015, [Internet], Available at: <http://odlucivanje.fon.bg.ac.rs/wp-content/uploads/Expert-Choice.pdf>, Retrieved: 16.05.2015.godine.

Kaurin, T., & Anucojić, D., 2012, Smernice za izbor alata digitalne forenzike, str. 715, *Infoteh*, Jahorina, Mart 21-23.

McClure, S., Scambray, J., & Kurtz, G., 2002, *Hakerske tajne - zaštita mrežnih sistema*, Beograd: Mikro knjiga, str. 614.

Ranđelović, D., 2011, *Poređenje komercijalnih i nekomercijalnih alata digitalne forenzike i njihova upotreba*, Beograd: Vojnotehnički institut, str. 112-113.

Simeunović, N., & Ristić, N., 2013, Digitalna forenzika u funkciji digitalnog računovodstva, str. 1009, *Infoteh*, Jahorina, Mart 20-22.

ПРИМЕНЕНИЕ МНОГОКРИТЕРИАЛЬНОГО ПРИНЯТИЯ РЕШЕНИЙ ПРИ ВЫБОРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ ФОРЕНЗИКИ

Деян Р. Станивукович[а], *Драган* М. Ранджелович[б]

[а] ВС Республики Сербия, Генштаб, Главное управление Военной полиции, Следственно-оперативное подразделение, г.Нови-Сад, Республика Сербия,

[б] Министерство внутренних дел Республики Сербия, Криминалистическо-полицейская академия, Кафедра информатики, г. Белград, Республика Сербия

ОБЛАСТЬ: компьютерные науки, информатика
ВИД СТАТЬИ: профессиональная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

В наше время почти не существует преступлений, раскрытие которых обошлось бы без цифровых доказательств. Так как объем носителей, хранящих цифровые данные ежедневно увеличивается, требуется больше времени на выявление и копирование (приобретение) цифровых доказательств. В этой связи, выбор соответствующих программных обеспечений цифровой форензики более чем актуален.

Выбор соответствующего программного обеспечения изначально включает сравнительный анализ двух или более программных обеспечений цифровой форензики, а также их оптимизацию. Целью сравнительного анализа программного обеспечения является определение и сравнение их реальной и сопоставимой производительности. Оптимизация производится с целью определения какое из программных обеспечений цифровой форензики обладает лучшей производительностью.

В данной статье представлен один из вариантов выбора программного обеспечения цифровой форензики, при применении последних достижений науки, касательно поддержки принятия решений на основании аналитического иерархического процесса (AHP), и компьютерной программы Expert Choice.

Ключевые слова: *судебно-программное обеспечение, цифровые экспертизы, эксперт выбор, оптимизация, цифровые доказательства, сравнительный анализ.*

PRIMENA VIŠEKRITERIJUMSKOG ODLUČIVANJA U IZBORU SOFTVERA DIGITALNE FORENZIKE

Dejan R. Stanivuković[a], *Dragan* M. Ranđelović[b]
[a] Vojska Srbije, Generalštab, Uprava Vojne policije, Kriminalističko-istražna grupa, Novi Sad, Republika Srbija,
[b] Ministarstvo unutrašnjih poslova Republike Srbije, Kriminalističko-policijska akademija, Katedra informatike, Beograd, Republika Srbija

OBLAST: računarske nauke, informatika
VRSTA ČLANKA: stručni članak
JEZIK ČLANKA: engleski

Sažetak:

U današnje vreme gotovo da nema krivičnog dela u čijem rasvetljavanju digitalni dokazi nemaju ključnu ulogu. Konstantno povećanje kapaciteta medija na kojima se skladište digitalni podaci neprestano povećava vreme neophodno za identifikaciju i kopiranje (akviziciju) digitalnih dokaza. S tim u vezi, izbor adekvatnog softvera digitalne forenzike sve više dobija na značaju.

Izbor adekvatnog softvera podrazumeva prethodnu uporednu analizu dva ili više softvera digitalne forenzike i proces optimizacije. Cilj uporedne analize ovih softvera jeste utvrđivanje i međusobno upoređivanje njihovih realnih i uporedivih performansi. Optimizacija ima za cilj da se utvrdi koji od softvera digitalne forenzike ima bolje performanse.

U ovom radu prikazana je jedna od mogućih varijanti izbora softvera digitalne forenzike, korišćenjem najsavremenijih naučnih dostignuća u podršci odlučivanju zasnovanih na metodi analitičko-hijerarhijskih procesa (AHP) i računarskom programu Expert Choice.

Ključne reči: *forenzički softver, digitalna forenzika, expert choice, optimizacija, digitalni dokaz, uporedna analiza.*

Paper received on / Дата получения работы / Datum prijema članka: 31. 08. 2015.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Datum dostavljanja ispravki rukopisa: 26. 02. 2016.
Paper accepted for publishing on / Дата окончательного согласования работы / Datum konačnog prihvatanja članka za objavljivanje: 28. 02. 2016.